

1 David. S. Casey, Jr., SBN 060768

2 *dcasey@cglaw.com*

3 Gayle M. Blatt, SBN 122048

4 *gmb@cglaw.com*

5 P. Camille Guerra, SBN 326546

6 *camille@cglaw.com*

7 **CASEY GERRY SCHENK**

8 **FRANCAVILLA BLATT & PENFIELD, LLP**

9 110 Laurel Street

10 San Diego, CA 92101

11 Tel: (619) 238-1811

12 Fax: (619) 544-9232

13 *Attorneys for Plaintiffs and*

14 *the Putative Classes*

15 *[Additional Counsel Listed on Signature Page]*

16 **UNITED STATES DISTRICT COURT**

17 **NORTHERN DISTRICT OF CALIFORNIA**

18 MICHAEL GREENSTEIN, CYNTHIA  
19 NELSON, and SINKWAN AU,  
20 individually and on behalf of themselves  
21 and all other persons similarly situated,

22 Plaintiffs,

23 v.

24 NOBLR RECIPROCAL EXCHANGE,

25 Defendant.

Case No. 4:21-cv-04537-JSW

**PLAINTIFFS' SECOND AMENDED  
CLASS ACTION COMPLAINT**

**Demand for Jury Trial**

26 Plaintiffs Michael Greenstein, Cynthia Nelson, and Sinkwan Au, individually,  
27 and on behalf of all others similarly situated, upon personal knowledge of facts  
28 pertaining to them and on information and belief as to all other matters, by and  
through undersigned counsel, hereby bring this Second Amended Class Action  
Complaint against Defendant Noblr Reciprocal Exchange and allege as follows:

## INTRODUCTION

1. Every year millions of Americans have their most valuable personal information stolen and sold online because of unauthorized data disclosures. Despite warnings about the severe impact of unauthorized data disclosures on Americans of all economic strata, companies still fail to put adequate security measures in place to prevent the unauthorized disclosure of private data about their customers or potential customers.

2. Defendant Noblr Reciprocal Exchange (“Defendant” or “Noblr”), provides insurance products, including car insurance, to Americans across the country. In doing so, it promises “[y]ou trust us with your information and we are committed to keeping that trust,” “the security of your personal information is extremely important to us” and further promises in bold lettering “[w]e do not share your data or information without your permission.”<sup>1</sup>

3. Noblr failed to meet these promises and its obligation to protect the sensitive personal information entrusted to it.

4. As reported by Noblr, on or about January 21, 2021, it “noticed unusual quote activity consisting of a spike in unfinished quotes through its instant quote webpage.” It launched an investigation and learned that “attackers may have initiated these quotes in order to steal driver’s license numbers which were inadvertently included in the page source code.”<sup>2</sup> This means that for an unknown period of time before and including January 21, 2021, the drivers’ license information of Plaintiffs and members of the class, who total almost a hundred thousand people, was publicly available on Noblr’s website via the publicly-viewable page source code, which is code underlying a website that can be seen by

---

<sup>1</sup> <https://www.noblr.com/privacy-policy/>

<sup>2</sup> <https://media.dojmt.gov/wp-content/uploads/noblr-notif.pdf> (last visited May 29, 2021).

1 anyone at the click of a button, and was also being stolen by hackers through  
2 automated bot processes designed to cull large numbers of driver's license numbers  
3 for sale and use by hackers.

4 5. As a corporation doing business in California, Noblr is legally required to  
5 protect the personal information ("PI") it gathers from unauthorized access and  
6 exfiltration.

7 6. As a result of Noblr's failure to provide reasonable and adequate data  
8 security, Plaintiffs' and the Class Members' PI— including their especially sensitive  
9 driver's license information—has been exposed to those who should not have access  
10 to it. And at least one of the named Plaintiffs has *already* been the victim of identity  
11 theft. All Plaintiffs and the Class are now at much higher risk of identity theft and  
12 for cybercrimes of all kinds, especially considering the highly valuable and sought-  
13 after private PI stolen here, and have suffered damages related to lost time, loss of  
14 privacy, and other harms.

### 15 THE PARTIES

16 7. Defendant Noblr Reciprocal Exchange is an unincorporated association  
17 domiciled in Colorado with its principal place of business in San Francisco,  
18 California. Noblr is an insurance provider currently providing insurance in Arizona,  
19 Colorado, Ohio, Louisiana, Maryland, Pennsylvania, New Mexico, and Texas, and  
20 has insurance licenses in all fifty states.

21 8. Plaintiff Michael Greenstein is a resident of Watchung, New Jersey. On  
22 or about May 2021, Plaintiff Greenstein received notice from Noblr that it  
23 improperly exposed his PI to unauthorized third parties. Plaintiff Greenstein never  
24 sought a quote for insurance of any sort from Defendant.

25 9. Plaintiff Cynthia Nelson is a resident of Watertown, Massachusetts. On  
26 or about May 2021, Plaintiff Nelson received notice from Noblr that it improperly  
27 exposed her PI to unauthorized third parties. Plaintiff Nelson never sought a quote  
28 for insurance of any sort from Defendant.

1           10. Plaintiff Sinkwan Au is a resident of Roslyn Heights, New York. On or  
2 about May 2021, Plaintiff Au received notice from Noblr that it improperly exposed  
3 her PI to unauthorized third parties. Plaintiff Au never sought a quote for insurance  
4 of any sort from Defendant.

5                                   **JURISDICTION AND VENUE**

6           11. Subject matter jurisdiction in this civil action is authorized pursuant to 28  
7 U.S.C. § 1332(d) because there are more than 100 Class Members, at least one class  
8 member is a citizen of a state different from that of Defendant, and the amount in  
9 controversy exceeds \$5 million, exclusive of interest and costs. The Court also has  
10 federal question jurisdiction under 28 U.S.C. § 1331 for the Drivers' Privacy  
11 Protection Act claims and supplemental jurisdiction over the state law claims  
12 pursuant to 28 U.S.C. § 1367.

13           12. This Court has personal jurisdiction over Defendant because it maintains  
14 its principal place of business in this District, is registered to conduct business in  
15 California, and has sufficient minimum contacts with California.

16           13. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because  
17 Defendant resides in this District and on information and belief, a substantial part of  
18 the events or omissions giving rise to Plaintiffs' and Class Members' claims  
19 occurred in this District.

20           14. Application of California law to this dispute is proper because  
21 Defendant's headquarters are in California, the decisions, actions, and/or  
22 circumstances that gave rise to the underlying facts at issue in this Complaint were  
23 presumably made or taken in California, and the action and/or inaction at issue  
24 emanated from California.

25                                   **INTRADISTRICT ASSIGNMENT**

26           15. Pursuant to Civil L.R. 3-1 (c) and (d), assignment to the San Francisco  
27 Division is proper because a substantial part of the conduct which gives rise to  
28 Plaintiffs' claims occurred in this district and specifically San Francisco County

where Defendant is headquartered.

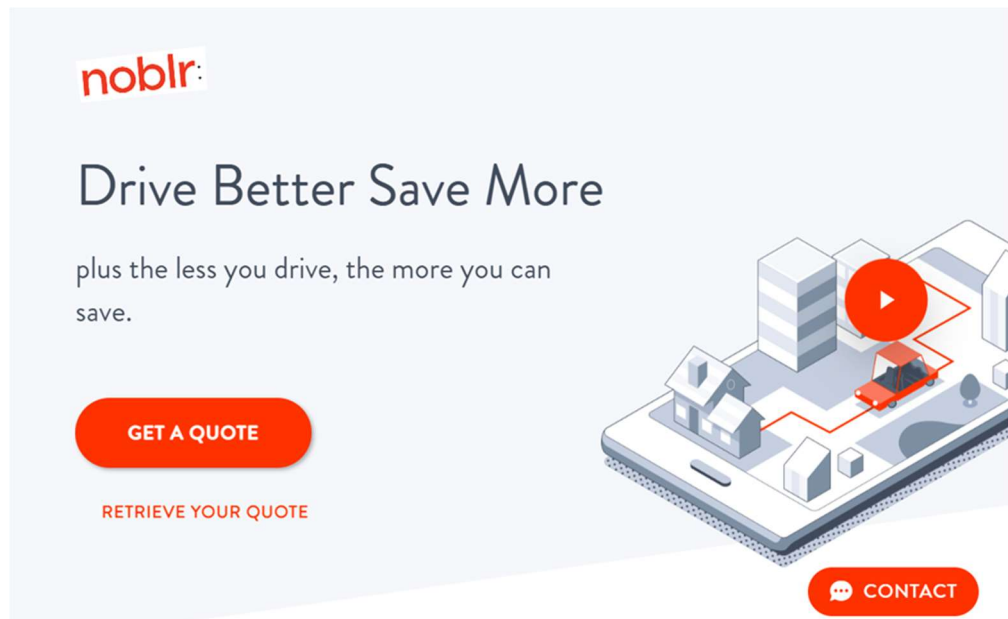
## **FACTUAL ALLEGATIONS**

### **A. Noblr collects PI and fails to provide adequate data security**

16. Noblr began as a car insurance start-up utilizing technology to provide a product to attract good drivers, “Using behaviour based pricing, Noblr calculated insurance premiums in real-time based on how a driver performs.”<sup>3</sup>

17. Noblr currently offers various types of insurance policies, including auto, renters, home and condo, and umbrella.<sup>4</sup>

18. Like other insurance providers, Noblr offers a public-facing insurance quoting platform for visitors on its website. Visitors to Noblr’s website can “Get A Quote” instantly after providing personal information.



19. Noblr’s quoting feature uses the information entered by the website’s visitor, combines it with additional information the system matches, and then automatically pulls information from a third-party to provide the visitor a quote.

<sup>3</sup> <https://www.artemis.bm/news/hudson-structured-invests-in-auto-insurtech-noblr/> (last visited May 29, 2021).

<sup>4</sup> <https://www.noblr.com/coverages/>

1           20. Specifically, Noblr’s quoting feature, which is still available on its  
2 website, asks a potential customer for a name, date of birth, and then an address.  
3 Once that information is entered, Noblr’s system auto-populates the quotation with  
4 driver’s license information and makes that information visible to the person  
5 entering the information on the Noblr quote website.

6           21. Noblr’s online quote website did not require verification that the person  
7 or automated process entering name, date of birth, and address information was the  
8 same person for whom the information was being entered. Instead, and  
9 unfortunately, Noblr’s online quote system was configured to allow anyone with a  
10 few basic bits of data to get Noblr’s system to auto-fill the remaining information,  
11 including driver’s license numbers, from its databases, and provide it without any  
12 further confirmation as to who was receiving the information, thus allowing hackers  
13 to steal that information.

14           22. In addition, Noblr put the driver’s license information it had in its  
15 possession – via motor vehicle records and third-party sources – in the source code  
16 of its website, which is publicly viewable at the click of a button. As a result, *even*  
17 *without the exploitation of hackers discovered by Noblr in 2021*, Noblr had  
18 intentionally put driver’s license information for at least 97,633 people, as reported  
19 by Noblr, including both Noblr customers and the general public, including  
20 Plaintiffs, on its website available for hackers to steal en masse.

21           23. On or around January 21, 2021, Noblr finally realized that its instant  
22 quote feature was being exploited by hackers who were using it to obtain the driver’s  
23 license numbers and addresses of Plaintiffs and the members of the Class, which  
24 includes many people who never applied for insurance with Noblr or were even  
25 aware of its existence.

26           24. This incident is referred to herein as the “Unauthorized Data Disclosure.”

27           25. The named Plaintiffs received a letter from Noblr entitled “Notice of  
28 Data Security Incident Involving Your Personal Data,” dated May 14, 2021. The

1 letter stated that their PI, detailed below, may have been compromised, and included  
2 the following:

3 **What Happened**

4 On January 21, 2021, Noblr's web team noticed unusual quote activity  
5 consisting of a spike in unfinished quotes through its instant quote web  
6 page. Noblr immediately launched an internal investigation. The initial  
7 investigation revealed that attackers may have initiated these quotes in  
8 order to steal driver's license numbers which were inadvertently  
9 included in the page source code.

10 As described above, the instant quote process works by taking personal  
11 data (name and date of birth) entered into the system and matching it  
12 with related information automatically pulled from a third-party to help  
13 provide a quote. The attackers appear to have already been in  
14 possession of the names and dates of birth of consumers, and then used  
15 that information to obtain additional personal information through  
16 Noblr's instant quote platform. Attackers could also have gone through  
17 the entire quote process to access personal information in the final  
18 policy application documents provided after obtaining a quote.

19 On January 25, 2021, following the initial discovery of unusual quote  
20 activity, Noblr's security team began blocking suspicious IP addresses.  
21 On January 27, 2021, when Noblr determined that the attackers were  
22 able to access driver's license numbers, Noblr altered its instant quote  
23 system to prevent further access by the attackers and took other steps  
24 to combat these attacks.

25 **What Information Was Involved**

26 Our records indicate that your name, driver's license number, and  
27 address may have been accessed.

28 **Actions We've Taken to Safeguard Your Information**

We take our responsibility to safeguard your personal information  
seriously. We immediately took steps to remedy the situation, including  
blocking suspicious IP addresses, revising rate limit thresholds to adjust  
specific traffic patterns, and altering the instant quote system to mask  
driver's license numbers in the source code and in the final application

1 page. In addition, we are developing and employing certain changes to  
 2 processes and protocols to prevent this type of event from happening  
 3 again.<sup>5</sup>

4 26. The Notice confirms that Plaintiffs became victims of the Unauthorized  
 5 Data Disclosure even though they did not have a prior relationship with Noblr,  
 6 Indeed the Notice advised that “you may be affected even if you have no  
 7 relationship with Noblr if your information, or the information of someone in your  
 8 household, was used by the attackers in connection with this incident.”

9 27. The Notice also confirms that at least 97,633 people were affected by the  
 10 Unauthorized Data Disclosure, and that driver’s license numbers, as well as non-  
 11 driver identification card numbers, were acquired.<sup>6</sup> And the Notice confirms that the  
 12 hackers *already had* PI about Plaintiffs and Class Members and used the  
 13 Defendant’s website to obtain and link additional PI, including driver’s license  
 14 numbers and addresses.<sup>7</sup>

15 28. After receiving Unauthorized Data Disclosure notice letters, it is  
 16 reasonable for Plaintiffs and Class Members in this case to believe that the risk of  
 17 future harm (including identity theft) is substantial and imminent, and to take steps  
 18 to mitigate that substantial risk of future harm. In fact, Noblr’s letter encourages  
 19 affected individuals to use the identity theft protection service it offers to Plaintiffs  
 20 and the Class to help protect their “identity from misuse” and that they should,  
 21 among other things, “regularly review statements from your accounts and  
 22 periodically obtain your credit report.”

---

23  
 24  
 25 <sup>5</sup> Noblr’s *Notice of Data Security Incident Involving Your Personal Information*, as  
 26 filed with the Maine Attorney General,  
 27 <https://apps.web.maine.gov/online/aevviewer/ME/40/c43bf2a1-cca9-45fa-81bf-47d299a7216d.shtml> (last visited on May 29, 2021).

28 <sup>6</sup> *Id.*

<sup>7</sup> *Id.*

**B. The PI exposed by Noblr as a result of its inadequate data security is highly valuable on the black market**

29. The information exposed by Noblr is very valuable to phishers, hackers, identity thieves and cyber criminals, especially at this time where unprecedented numbers of criminals are filing fraudulent unemployment benefit claims and driver's license information is uniquely connected to the ability to file a fraudulent unemployment benefit claim.

30. Indeed, these hackers often aggregate information taken from these breaches on users to build profiles on individuals. These profiles combine publicly available information with information discovered in previous data breaches and exploited vulnerabilities. There are few data breaches that provide a comprehensive snapshot of any one individual person. Unique and persistent identifiers such as Social Security Numbers, driver's license numbers, usernames, and financial account numbers (e.g., credit cards, insurance policy numbers, etc.) are critical to easily forging an identity. When not all information is available, the information that is stolen is used to socially engineer a victim into providing additional information so a "fullz"<sup>8</sup> profile can be obtained.

31. For example, a health care system and a retail store point-of-sale system may have two unrelated data breaches where an individual's information is taken. The individual's driver's license may not be in either of those data bases, but after the Unauthorized Data Disclosure, a threat actor could have improved the profile and added a driver's license number. The value of that profile would allow such crimes as identity theft, financial crimes, and even illegal voting that would not previously have been possible.

---

<sup>8</sup> "Fullz" is slang used by threat actors and various criminals meaning "full information," a complete identity profile or set of information on any entity or individual.

1           32. There is no legitimate or legal reason for anyone to use Noblr's  
2 inadequate website security to acquire driver's license information for 97,833 people.  
3 The only reason is for immediate or eventual malicious intent, since no one would go  
4 to the trouble of obtaining data that had no value. Any non-public data, especially  
5 government issued identification numbers like a driver's license or non-driver's  
6 identification number, has criminal value. On the darknet markets, a driver's license,  
7 combined with the full name and state issued, is a sought-after data point. Darknet  
8 markets are a downstream "flea market" for data to be sold, usually not by the original  
9 threat actor or criminal group. It is a dumping ground, usually after the data has been  
10 exploited.

11           33. The value of stolen driver's license information currently has a darknet  
12 market (DNM) value of \$1 per license. This was re-verified on March 3, 2022,  
13 accessing several DNM using a trusted identity. Social Security Numbers, once  
14 considered the "gold standard" of identity fraud, are also selling for \$1 per value in  
15 those same markets. This illustrates the value of driver's license information to  
16 cybercriminals and people committing identity fraud. According to popular darknet  
17 markets, cyber criminals value driver's licenses equally to Social Security Numbers.

18           34. In some ways, driver's license numbers are even more attractive than  
19 Social Security Numbers to threat actors and more dangerous to the consumer when  
20 compromised. Unlike a Social Security Number, a driver's license number isn't  
21 monitored as closely, so it can potentially be used in ways that won't immediately  
22 alert the victim. Threat actors know this as well. Because driver's licenses contain, or  
23 can be used to gain access to, uniquely qualifying and comprehensive identifying  
24 information such as eye color, height, weight, sex, home address, medical or visual  
25 restrictions, and living will/health care directives, most insurance and credit agencies  
26 highly recommend that immediate notice, replacement, and identity theft protections  
27  
28

are put in place for a minimum of 3 years.<sup>9</sup> Most cyber experts, including Enterprise Knowledge Partners, recommend five years or more.

35. Stolen driver's licenses can be used (alone or in combination with other information) by malicious actors to accomplish the following:

- Apply for credit cards
- Apply for financial loans (especially student loans)
- Open bank accounts
- Obtain or create fake driver's licenses
  - Given to police for tickets
  - Provided to accident victims
  - Collect government unemployment benefits
  - Create and sell underage fake IDs
- Replace/access account information on:<sup>10</sup>
  - LinkedIn
  - Facebook/Meta
  - WhatsApp
  - Instagram
- Obtain a mobile phone
- Dispute or prove a SIM swap
- Redirect U.S. mail
- Apply for unemployment benefits

---

<sup>9</sup> See, e.g., <https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/>; <https://us.norton.com/internetsecurity-id-theft-lost-or-stolen> (last accessed Mar. 7, 2022).

<sup>10</sup> A copy of a driver's license with a validated driver's license number is required to recover an online account or to have a suspected cloned / fraudulent account removed. See, e.g., <https://www.linkedin.com/pulse/facebook-coerces-victims-fraud-upload-birth-voter-id-card-scheinker/> (last accessed Mar. 7, 2022).

- Undocumented aliens may use them as a method to gain access to the U.S., and claim a lost or stolen passport
- Create a fake license as a baseline to obtain a Commercial Driver's License
- File tax returns or gain access to filed tax returns<sup>11</sup>
- Engage in phishing and other social engineering scams

36. The process that was used to extract the data from Noblr's website based on its flaws and lack of security was likely automated. The Notice seemingly confirms this when it notes that the Unauthorized Data Disclosure was discovered when "Noblr's web team noticed *unusual quote activity consisting of a spike* in unfinished quotes through its instant quote web page" (emphasis added) and confirmed that threat actors like those described herein were at fault as "attackers appear to have already been in possession of the names and dates of birth of consumers, and then used that information to obtain additional personal information through Noblr's instant quote platform."

37. Unsecured sites that contain or transmit PI, such as a driver's license, require notice to consumers when the data is stolen because it can be used to perform identity theft and other types of fraud. A threat actor is usually motivated by financial or political gain before it exerts time, and skill to compromise and exfiltrate. Over time, identity thieves have systematized their criminal activities to gather important pieces of a synthetic identity from multiple breaches and sources. The theft of a driver's license number is no less valuable in that endeavor than the theft of a Social Security Number, as demonstrated by these two unique identifiers carrying the same price on the darknet, and by the fact that the identity thieves have demonstrated a systematic and businesslike process for collecting these stolen driver's license numbers in this Unauthorized Data Disclosure and others committed

---

<sup>11</sup> <https://blog.rodefermoss.com/keeping-your-drivers-license-number-safe-may-prevent-tax-fraud>

1 against insurers. Cybercrime has been on the rise for the past decade and continues  
2 to climb exponentially; as of 2013 it was being reported that nearly one out of four  
3 data breach notification recipients become a victim of identity fraud.<sup>12</sup>

4 38. As alleged above, stolen PI is often trafficked on the “dark web,” a  
5 heavily encrypted part of the Internet that is not accessible via traditional search  
6 engines. Law enforcement has difficulty policing the dark web due to this  
7 encryption, which allows users and criminals to conceal identities and online  
8 activity.

9 39. When malicious actors infiltrate companies and copy and exfiltrate the PI  
10 that those companies store, or have access to, that stolen information often ends up  
11 on the dark web because the malicious actors buy and sell that information for  
12 profit.<sup>13</sup>

13 40. For example, when the U.S. Department of Justice announced its seizure  
14 of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which  
15 concerned stolen or fraudulent documents that could be used to assume another  
16 person’s identity. Other marketplaces, similar to the now-defunct AlphaBay, “are  
17 awash with [PI] belonging to victims from countries all over the world. One of the  
18 key challenges of protecting PI online is its pervasiveness. As unauthorized data  
19 disclosures in the news continue to show, PI about employees, customers and the  
20 public is housed in all kinds of organizations, and the increasing digital  
21 transformation of today’s businesses only broadens the number of potential sources  
22 for hackers to target.”<sup>14</sup>

---

23  
24 <sup>12</sup> Pascual, Al, “2013 Identity Fraud Report: Data Breaches Becoming a Treasure  
25 Trove for Fraudsters,” *Javelin* (Feb. 20, 2013).

26 <sup>13</sup> *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce, Dec. 28,  
27 2020, available at: [https://www.identityforce.com/blog/shining-light-dark-web-](https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring)  
28 [identity-monitoring](https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring) (last visited May. 29, 2021).

<sup>14</sup> *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor,

41. The PI of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200<sup>15</sup> Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.<sup>16</sup> (Note: the prices can vary depending on the point in the chain – verified identities may sell for higher prices early in the chain, then for the lower prices described above when they reach the “flea market sites.”) The information compromised in the Unauthorized Data Disclosure is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. And the information compromised in the Unauthorized Data Disclosure can be used to *open* fraudulent bank accounts and credit and debit cards, compounding the identity theft and cycle of black market sales detailed above. The information compromised in this Unauthorized Data Disclosure is also more valuable because driver’s license numbers, non-driver’s identification numbers, and addresses are difficult and likely highly problematic, to change.

42. Recently, Forbes writer Lee Mathews reported on Geico’s similar unauthorized data disclosure wherein the hackers also targeted driver’s license numbers, “Hackers harvest license numbers because they’re a very valuable piece of information. A driver’s license can be a critical part of a fraudulent, synthetic identity – which go for about \$1200 on the Dark Web. On its own, a forged license

---

April 3, 2018, *available at*: <https://www.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/> (last visited June 10, 2021).

1 can sell for around \$200.”<sup>17</sup>

2 43. National credit reporting company, Experian, blogger Sue Poremba also  
3 emphasized the value of driver’s license to thieves and cautioned:

4 If someone gets your driver’s license number, it is also  
5 concerning because it’s connected to your vehicle registration  
6 and insurance policies, as well as records on file with the  
7 Department of Motor Vehicles, place of employment (that keep  
8 copy of your driver’s license on file), doctor’s office, government  
9 agencies, and other entities. Having access to that one number  
10 can provide an identity thief with several pieces of information  
11 they want to know about you. Next to your Social Security  
12 number, your driver’s license is one of the most important pieces  
13 to keep safe from thieves.<sup>18</sup>

14 44. In fact, according to CPO Magazine, which specializes in news, insights  
15 and resources for data protection, privacy and cyber security professionals, “[t]o  
16 those unfamiliar with the world of fraud, *driver’s license numbers might seem like a*  
17 *relatively harmless piece of information to lose if it happens in isolation*. Tim  
18 Sadler, CEO of email security firm Tessian, points out why *this is not the case* and  
19 why these numbers are very much sought after by cyber criminals: “It’s a gold mine  
20 for hackers. With a driver’s license number, bad actors can manufacture fake IDs,  
21 slotting in the number for any form that requires ID verification, or use the  
22 information to craft curated social engineering phishing attacks. . . . bad actors may  
23 be using these driver’s license numbers to fraudulently apply for unemployment  
24 benefits in someone else’s name, a scam proving especially lucrative for hackers as

---

25 <sup>17</sup> Lee Mathews, *Hackers Stole Customers’ License Numbers from Geico in Months-*  
26 *Long Breach*, (April 20, 2021), available at:  
27 [https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-](https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3066c2218658)  
28 [license-numbers-from-geico-in-months-long-breach/?sh=3066c2218658](https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3066c2218658) (last visited  
May 29, 2021).

<sup>18</sup> Sue Poremba, *What should I do If My Driver’s License Number is Stolen?* (Oct. 24,  
2018), available at: [https://www.experian.com/blogs/ask-experian/what-should-i-do-](https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/)  
[if-my-drivers-license-number-is-stolen/](https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/) (last visited May 29, 2021).

1 unemployment numbers continue to soar. . . . In other cases, a scam using these  
 2 driver’s license numbers could look like an email that impersonates the DMV,  
 3 requesting the person verify their driver’s license number, car registration or  
 4 insurance information, and then inserting a malicious link or attachment into the  
 5 email.” (emphasis added).

6 45. Drivers’ license numbers have been taken from auto-insurance providers  
 7 by hackers in other circumstances, including Geico, American Family, Farmers, and  
 8 Midvale all in 2021, indicating both that this particular form of PI is in high demand  
 9 and also that Noblr knew or had reason to know that its security practices were of  
 10 particular importance to safeguard consumer data.<sup>19</sup>

11 46. In fact, when Geico announced that its online quoting platform—which is  
 12 nearly identical to Noblr’s—was subject to a near-identical breach, its data breach  
 13 notice filed with the California Attorney General explicitly stated that GEICO had  
 14 “reason to believe that this information could be used to fraudulently apply for  
 15 unemployment benefits in your name.”<sup>20</sup>

16 47. Further, an article on TechCrunch explains that it is driver’s license or  
 17 non-driver’s identification numbers themselves that are the critical missing link for a  
 18 fraudulent unemployment benefits application: “Many financially driven criminals  
 19 target government agencies using stolen identities or data. But many U.S. states  
 20 require a government ID — like a driver’s license — to file for unemployment  
 21

---

22 <sup>19</sup> See United States Securities and Exchange Commission Form 8-K for INSU  
 23 Acquisition Corp. II (Feb. 1, 2021),  
 24 [https://www.sec.gov/Archives/edgar/data/1819035/000121390021005784/ea134248-](https://www.sec.gov/Archives/edgar/data/1819035/000121390021005784/ea134248-8k_insuacquis2.htm?d=1819035-01022021)  
 25 [8k\\_insuacquis2.htm?d=1819035-01022021](https://www.sec.gov/Archives/edgar/data/1819035/000121390021005784/ea134248-8k_insuacquis2.htm?d=1819035-01022021) (accessed Apr. 27, 2021) (announcing a  
 26 merger with auto-insurance company MetroMile, Inc., an auto-insurer, which  
 27 announced a drivers’ license number Data Disclosure on January 19, 2021); Ron  
 28 Lieber, *How Identity Thieves Took My Wife for a Ride*, N.Y. TIMES (Apr. 27, 2021)  
 (describing a scam involving drivers’ license numbers and Progressive Insurance).

<sup>20</sup> See [https://www.documentcloud.org/documents/20618953-geico-data-breach-](https://www.documentcloud.org/documents/20618953-geico-data-breach-notice)  
[notice](https://www.documentcloud.org/documents/20618953-geico-data-breach-notice) (GEICO notice filed with California Attorney General dated April 9, 2021)

benefits. To get a driver's license number, fraudsters take public or previously breached data and exploit weaknesses in auto insurance websites to obtain a customer's driver's license number. That allows the fraudsters to obtain unemployment benefits in another person's name."<sup>21</sup> Driver's license number are thus the critical piece of data needed to apply fraudulently for unemployment benefits.

48. For example, the New York State Department of Financial Services issued an industry letter on February 16, 2021, stating that they had "recently learned of a systemic and aggressive campaign to exploit cybersecurity flaws in public-facing websites to steal [NPI, including] websites that provide an instant quote. . . . [I]t received reports from two auto insurers in late December 2020 and early January 2021, that cybercriminals were targeting their websites that offer instant [] quotes [] to seal unredacted driver's license numbers. . . . DFS has confirmed that, at least in some cases, this stolen information has been used to submit fraudulent claims for pandemic and unemployment benefits."<sup>22</sup>

49. Once PI is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details, or to fraudulently manufacture new accounts for access and sale. This can lead to additional PI being harvested from the victim, as well as PI from family, friends and colleagues of the original victim.

50. According to the FBI's Internet Crime Complaint Center (IC3) 2019

---

<sup>21</sup> Zach Whittaker, *Geico Admits Fraudsters Stole Customers' Driver's License Numbers for Months*, TechCrunch (Apr. 19, 2021), <https://techcrunch.com/2021/04/19/geico-driver-license-numbers-scraped/#:~:text=To%20get%20a%20driver's%20license,benefits%20in%20another%20person's%20name> (last accessed Mar. 2, 2022).

<sup>22</sup> [https://www.dfs.ny.gov/industry\\_guidance/industry\\_letters/il20210216\\_cyber\\_fraud\\_alert](https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert) (last accessed March 7, 2022).

Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than \$3.5 billion in losses to individuals and business victims.

51. Further, according to the same report, “rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good.” Defendant did not rapidly report to Plaintiffs and Class Members that their PI had been stolen. It took Noblr almost four months to do so. This means that for those four months, it was not possible for law enforcement to stop identity theft experienced by Plaintiffs and members of the class, and also prevented Plaintiffs and members of the class from starting to take mitigative steps to protect themselves from their substantial and incremental increased risk of identity theft.

52. Victims of drivers’ license number theft also often suffer unemployment benefit fraud, as discussed above, as well as harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

53. Unauthorized data disclosures facilitate identity theft as hackers obtain consumers’ PI and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers’ PI to others who do the same.

54. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the “GAO Report”) that criminals use PI to open financial accounts, receive government benefits, and make purchases and secure credit in a victim’s name.<sup>23</sup> The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to

---

<sup>23</sup> See Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), available at <http://www.gao.gov/assets/270/262899.pdf> (last visited May 29, 2021).

1 become aware of the fraud, and can adversely impact the victim’s credit rating in the  
 2 meantime. The GAO Report also states that identity theft victims will face  
 3 “substantial costs and inconveniences repairing damage to their credit records . . .  
 4 [and their] good name.”<sup>24</sup>

5 **C. Noblr was on notice of the sensitivity and private nature of the PI it**  
 6 **utilized for insurance quotes and its duty to safeguard it**

7 55. “Insurance companies are desirable targets for cyber attackers because  
 8 they work with sensitive data.”<sup>25</sup> In fact, according to the Verizon 2020 Data Breach  
 9 Investigations Report there were 448 confirmed data breaches in the financial and  
 10 insurance industries.<sup>26</sup>

11 56. Noblr claims it “uses commercially reasonable and industry standard  
 12 administrative, technical, personnel, and physical security measures designed to  
 13 protect the information we collect about you from loss, theft, and unauthorized use,  
 14 disclosure, or modification,” however, those safety and security measures were  
 15 insufficient. And while Noblr states that the information is protected in an encrypted  
 16 environment,<sup>27</sup> it was not. The weakness in Noblr’s system allowed access and  
 17 ability to exfiltrate Plaintiffs’ and the Class Members’ addresses and driver’s license  
 18 numbers.

19 57. In addition, Noblr is an insurance company that sells auto insurance and  
 20 uses motor vehicle records to verify identities and underwrite policies. Its  
 21 underwriting and other insurance activities are explicitly subject to the DPPA, which  
 22

---

23 <sup>24</sup> *Id.*

24 <sup>25</sup> Data Protection Compliance for the Insurance Industry (October 7, 2020), *available*  
 25 *at:* [https://www.ekransystem.com/en/blog/data-protection-compliance-insurance-](https://www.ekransystem.com/en/blog/data-protection-compliance-insurance-industry)  
 26 [industry](https://www.ekransystem.com/en/blog/data-protection-compliance-insurance-industry) (last visited May 29, 2021).

26 <sup>26</sup> Verizon 2020 Data Breach Investigations Report (2020), *available at:*  
 27 [https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/](https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf)  
 28 [2020-data-breach-investigations-report.pdf](https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf) (last visited May 29, 2021).

<sup>27</sup> *Id.*

1 was enacted in 1994 and has been in effect for Noblr’s entire existence as a  
 2 company, as Noblr was founded in 2017.<sup>28</sup>

3 58. Even among insurance companies who sell auto policies, Noblr was  
 4 uniquely situated to know it was using PI and other sensitive information in its  
 5 business. Noblr’s business model is predicated on using behavioral information and  
 6 ongoing information about customers to keep costs for policies down by rewarding  
 7 good driving. According to Noblr investors, “Using behaviour based pricing, Noblr  
 8 calculated insurance premiums in real-time based on how a driver performs. The  
 9 company says good drivers can save up to 51% on their auto insurance premiums,  
 10 while its highly personalised pricing model help directly incentivise better driving  
 11 and as a result safer roads as well.”

12 59. In addition, Noblr consciously uses PI and information about customers  
 13 on an *ongoing* basis. As CEO Gary Tolman noted, “We believe good drivers deserve  
 14 fairer and more transparent car insurance rates, along with the tools they need to  
 15 continuously improve their driving to earn lower premiums and create safer roads  
 16 for all.”<sup>29</sup> Noblr’s continual collection of PI in the form of customer information,  
 17 driving records, accident reports, and other motor vehicle information, along with its  
 18 insurance underwriting and business collection of driver’s license and other motor  
 19 vehicle information, put it in the position of knowing that it was obligated to protect  
 20 the privacy of its customers and potential customers like Plaintiffs and members of  
 21 the class.

22 **D. Noblr failed to comply with Federal Trade Commission requirements**

23 60. Federal and State governments have established security standards and  
 24 issued recommendations to minimize unauthorized data disclosures and the resulting  
 25

26 <sup>28</sup> See Bloomberg Profile for Gary Charles Tolman, Founder and CEO of Noblr Inc,  
 27 <https://www.bloomberg.com/profile/person/3362775> (last visited Mar. 3, 2022)  
 (listing Noblr’s date of incorporation as October 17, 2017).

28 <sup>29</sup> See *supra* note 3.

1 harm to individuals and financial institutions. The Federal Trade Commission  
 2 (“FTC”) has issued numerous guides for businesses that highlight the importance of  
 3 reasonable data security practices. According to the FTC, the need for data security  
 4 should be factored into all business decision-making.<sup>30</sup>

5 61. In 2016, the FTC updated its publication, *Protecting Personal*  
 6 *Information: A Guide for Business*, which established guidelines for fundamental  
 7 data security principles and practices for business.<sup>31</sup> Among other things, the  
 8 guidelines note businesses should properly dispose of personal information that is no  
 9 longer needed; encrypt information stored on computer networks; understand their  
 10 network’s vulnerabilities; and implement policies to correct security problems. The  
 11 guidelines also recommend that businesses use an intrusion detection system to  
 12 expose a breach as soon as it occurs; monitor all incoming traffic for activity  
 13 indicating someone is attempting to hack the system; watch for large amounts of  
 14 data being transmitted from the system; and have a response plan ready in the event  
 15 of a breach.<sup>32</sup>

16 62. Also, the FTC recommends that companies limit access to sensitive data;  
 17 require complex passwords to be used on networks; use industry-tested methods for  
 18 security; monitor for suspicious activity on the network; and verify that third-party  
 19 service providers have implemented reasonable security measures.<sup>33</sup>

20 63. Highlighting the importance of protecting against unauthorized data  
 21 disclosures, the FTC has brought enforcement actions against businesses for failing  
 22

---

23 <sup>30</sup> See Federal Trade Commission, *Start With Security* (June 2015), available at:  
 24 [https://www.ftc.gov/system/files/documents/plain-language/pdf0205-](https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf)  
 25 [startwithsecurity.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf) (last visited May 29, 2021).

26 <sup>31</sup> See Federal Trade Commission, *Protecting Personal Information: A Guide for*  
 27 *Business* (Oct. 2016), available at [https://www.ftc.gov/system/files/documents/plain-](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)  
 28 [language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last visited May 29, 2021).

<sup>32</sup> *Id.*

<sup>33</sup> Federal Trade Commission, *Start With Security*, *supra* footnote 25.

1 to adequately and reasonably protect PI, treating the failure to employ reasonable  
 2 and appropriate measures to protect against unauthorized access to confidential  
 3 consumer data as an unfair act or practice prohibited by Section 5 of the Federal  
 4 Trade Commission Act (“FTC Act”), 15 U.S.C. § 45. Orders resulting from these  
 5 actions further clarify the measures businesses must take to meet their data security  
 6 obligations.<sup>34</sup>

7 64. Through negligence in securing Plaintiffs’ and Class Members’ PI and  
 8 allowing the thieves to utilize its instant quote website platform to obtain access and  
 9 exfiltrate individuals’ PI, Noblr failed to employ reasonable and appropriate  
 10 measures to protect against unauthorized access to Plaintiffs’ and the Class  
 11 Members’ PI. Noblr’s data security policies and practices constitute unfair acts or  
 12 practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, and violate the  
 13 Gramm-Leach-Bliley Act (“GLB Act”), 15 U.S.C. § 6801.

#### 14 **E. Noblr Contravenes the Purpose of the Driver’s Privacy Protection Act**

15 65. Prior to the enactment of the Driver’s Privacy Protection Act, Congress  
 16 found that most states freely turned over DMV information to whomever requested  
 17 it with only few restrictions. 137 Cong. Rec. 27,327 (1993).

18 66. Due to this lack of restrictions, Congress grew concerned that potential  
 19 criminals could easily access home addresses and telephone numbers of potential  
 20 victims. 140 Cong. Rec. 7929 (1994) (statement of Rep. Porter Goss).

21 67. These concerns did, in fact, materialize in the occurrence of crime,  
 22 harassment, and stalking. Most notably, in 1989, a stalker shot and killed Rebecca  
 23 Schaeffer, an upcoming actor, after obtaining her unlisted home address from the  
 24 California DMV. 137 Cong. Rec. 27,327 (1993). In advocating for the DPPA,  
 25

---

26  
 27 <sup>34</sup> Federal Trade Commission, *Privacy and Security Enforcement Press Releases*,  
 28 available at <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement> (last visited Jan. 8, 2021).

Representative Jim Moran (D-VA) recounted thieves using information from the DMV to learn home addresses and commit burglary and theft. 137 Cong. Rec. 27,327 (1993). Similarly, Senator Barbara Boxer (D-CA) explained how a man used the DMV to obtain the home addresses of several young women and sent them harassing letters. 39 Cong. Rec. 29,466 (1993). In another instance, a woman who visited a clinic that performed abortions found black balloons outside her home after a group of anti-abortion activists sought to harass her upon seeing her car in the clinic's parking lot. 139 Cong. Rec. 29,462 (1993) (statement of Sen. Chuck Robb).

68. In light of public outrage over the Schaeffer murder and growing concern for the threat to public safety that free access to DMV records posed, Congress enacted the DPPA "to protect the personal privacy and safety of licensed drivers consistent with the legitimate needs of business and government." S. Res. 1589, 103rd Cong. §1(b), 139 Cong. Rec. 26,266 (1993) (enacted).

69. Additionally, in enacting the DPPA, Congress was motivated by its "[c]oncern[] that personal information collected by States in the licensing of motor vehicle drivers was being released – even sold – with resulting loss of privacy for many persons." *Akkawi v. Sadr*, 2:20-CV-01034-MCE-AC, 2021 WL 3912151, at \*4 (E.D. Cal. Sept. 1, 2021) (citing *Maracich v. Spears*, 570 U.S. 48, 51–52 (2013) (alterations in original)). The sale of private information like driver's license numbers and other motor vehicle records was the exact impetus for the DPPA's passage.

70. As such, Congress sought to expressly prohibit "disclosing personal information obtained by the department in connection with a motor vehicle record." *Chamber of Commerce of United States v. City of Seattle*, 274 F. Supp. 3d 1140, 1154 (W.D. Wash. 2017). Driver's license numbers are thus explicitly listed as "personal information" from "motor vehicle records" under the DPPA. *See* 18 U.S.C. 2725(1).

71. By making the PI of Plaintiffs and the Class publicly available, Noblr ran

1 afoul the purpose of DPPA, and threatened the privacy and safety of licensed  
 2 drivers, for whose protection the statute was enacted. Noblr's actions constituted a  
 3 concrete injury and particularized harm to Plaintiffs and members of the Class, that  
 4 would not have happened but for Noblr's failure to follow the DPPA. Plaintiffs  
 5 were harmed by the public disclosure of their private facts in addition to the other  
 6 harms enumerated herein.

7 **F. Noblr's Failure to Secure Driver's License Information on its Website**  
 8 **Independently Violates the DPPA and Harmed Plaintiffs and the Class**

9 72. In addition to allowing driver's license numbers to be queried at will by  
 10 hackers for at least the period of time identified by Noblr in the Notice received by  
 11 Plaintiffs, Noblr's privacy violations of Plaintiffs and members of the class and  
 12 public disclosure of private facts like driver's license information was far more  
 13 egregious than even other recent disclosures of driver's license information by  
 14 insurance companies. This is because Noblr's Notice admits that it placed the  
 15 driver's license information of an untold number of potential customers *in the source*  
 16 *code of its website*, which is *publicly available*, for some unknown period of time up  
 17 to and until at least January 27, 2021.

18 73. "Every major Internet browser allows users to view the HTML source  
 19 code of any web page they visit." While the method of access varies by web  
 20 browser, source code information is a part of a website that is public and routinely  
 21 visited by journalists, the public, and hackers alike. For example, on Google  
 22 Chrome, any user can press "Ctrl + U" and the source code will appear, or right-  
 23 click on a blank part of the web page and select "View page source."<sup>35</sup>

---

24  
 25 <sup>35</sup> See Computer Hope, Free computer help since 1998, *How to View the HTML*  
 26 *source code of a web page*,  
 27 <https://www.computerhope.com/issues/ch000746.htm#:~:text=Method%20-,Right%2Dclick%20a%20blank%20part%20of%20the%20web%20page%20and,sour,ce%20code%20of%20a%20page> (last accessed Mar. 2, 2022).  
 28

74. Website source code is a routine source for both legitimate and illegitimate seekers of information. For example, in October 2021, reporter Josh Renaud reported that the State of Missouri’s “Department of Elementary and Secondary Education website source code had exposed the social security numbers of over 100,000 school teachers, administrators, and counselors. He published the story only after he’d reported the problem to the state and the vulnerability had been resolved.” He did so by looking at the publicly-available, unencrypted source code of the state website. As an article explaining the situation noted, “A website’s source code is typically available to anyone using a web browser. While scraping it requires some technical knowledge, just looking at it is as simple as opening the “Developer Tools” option available in nearly every web browser, including Chrome, Safari, Firefox, and Edge. If you want, you can go look at The Verge’s source code right now.”<sup>36</sup>

75. As the FBI noted in the situation involving the state of Missouri above, when a company like Noblr puts unencrypted PI in the source code of the website, that is not a network intrusion; it’s a failure by the company, an instance where a database is “misconfigured,” and thus would “allow[] open source tools to be used to query data that should not be public.”<sup>37</sup>

76. Here, Noblr’s Notice states that “The initial investigation revealed that attackers may have initiated these quotes in order to steal driver’s license numbers

---

<sup>36</sup> Alex Cranz, *The Governor of Missouri Still Doesn’t Know How Websites Work*, The Verge (Dec. 31, 2021), <https://www.theverge.com/2021/12/31/22861188/missouri-governor-mike-parson-hack-website-source-code> (last accessed Mar. 3, 2022).

<sup>37</sup> Jack Suntrup, *Missouri Officials Planned to Thank Post-Dispatch Before Threatening Newspaper, Emails Show*, St. Louis Post-Dispatch (Dec. 3, 2021), [https://www.stltoday.com/news/local/govt-and-politics/missouri-officials-planned-to-thank-post-dispatch-before-threatening-newspaper-emails-show/article\\_0f6c5288-cd11-569c-804e-9b280e9c1e68.html](https://www.stltoday.com/news/local/govt-and-politics/missouri-officials-planned-to-thank-post-dispatch-before-threatening-newspaper-emails-show/article_0f6c5288-cd11-569c-804e-9b280e9c1e68.html) (last accessed Mar. 3, 2022).

1 which were inadvertently included in the page source code.” Thus, driver’s license  
 2 information was both unencrypted and publicly available on its website, and also  
 3 queried in a manner that indicates was designed to be used for theft.

4 77. Source code is created intentionally by a company as part of its creation  
 5 and maintenance of a website. Noblr wrote, created, and updated the source code on  
 6 its website over the course of its existence as a company, and as evidenced by its  
 7 Notice, which outlined changes made to the Noblr website after the Unauthorized  
 8 Data Disclosure.

9 78. None of Plaintiffs or members of the class authorized Noblr to place their  
 10 unencrypted driver’s license or non-driver’s identification numbers on their website  
 11 in the source code, and doing so is not a permissible use of such information under  
 12 the DPPA. The inclusion of such information on Noblr’s website also constitutes the  
 13 public disclosure of private facts and an invasion of privacy for Plaintiffs and  
 14 members of the class.

15 **G. Plaintiffs’ attempts to secure their PI after the breach**

16 **Plaintiff Greenstein**

17 79. In May 2021, Plaintiff Greenstein received notice from Noblr dated May  
 18 14, 2021 (“Notice Letter”). The Notice Letter informed him of the Unauthorized  
 19 Data Disclosure and that his driver’s license number and address may have been  
 20 accessed. Plaintiff Greenstein was not a customer of Noblr and had not requested an  
 21 insurance quote from Defendant.

22 80. Plaintiff Greenstein researched his options to respond to the theft of his  
 23 driver’s license. He spent and continues to spend additional time reviewing his credit  
 24 monitoring service results and reports from other online resources concerning the  
 25 security of his identity and financial information. This is time Plaintiff Greenstein  
 26 otherwise would have spent performing other activities, such as his job and/or  
 27 leisurely activities for the enjoyment of life.

28 81. Plaintiff Greenstein has never knowingly transmitted unencrypted PI

1 over the internet or any other unsecured source. He deletes any and all electronic  
2 documents containing his PI and destroys any documents that contain any of his PI,  
3 or that may contain any information that could otherwise be used to compromise his  
4 PI. Plaintiff Greenstein has not received a notice that his driver's license number  
5 was compromised in any other data breach or unauthorized data disclosure.

6 82. Plaintiff Greenstein suffered actual injury from having his PI exposed as  
7 a result of the Unauthorized Data Disclosure including, but not limited to: (a)  
8 damages to and diminution in the value of his PI—a form of intangible property; (b)  
9 loss of his privacy; and (c) imminent and impending injury arising from the  
10 increased risk of fraud and identity theft.

11 83. As a result of the Unauthorized Data Disclosure, Plaintiff Greenstein  
12 will continue to be at heightened risk for financial fraud, future identity theft, other  
13 forms of fraud, and the attendant damages, for years to come.

14 **Plaintiff Nelson**

15 84. In May 2021, Plaintiff Nelson received notice from Noblr dated May 14,  
16 2021 ("Notice Letter"). The Notice Letter informed her of the Unauthorized Data  
17 Disclosure and that her driver's license number and address may have been  
18 accessed. Plaintiff Nelson was not a customer of Noblr and had not requested an  
19 insurance quote from Defendant.

20 85. As a result, Plaintiff Nelson notified her bank and financial planner of the  
21 Unauthorized Data Disclosure. She also contacted her local police department.

22 86. Plaintiff Nelson researched her options to respond to the theft of her  
23 driver's license. She spent and continues to spend additional time reviewing her  
24 credit monitoring service results and reports from other online resources concerning  
25 the security of her identity and financial information. This is time Plaintiff Nelson  
26 otherwise would have spent performing other activities, such as her job and/or  
27 leisurely activities for the enjoyment of life.

28 87. Plaintiff Nelson has never knowingly transmitted unencrypted PI over the

internet or any other unsecured source. She deletes any and all electronic documents containing her PI and destroys any documents that contain any of her PI, or that may contain any information that could otherwise be used to compromise her PI. Plaintiff Nelson has not received a notice that her driver's license number was compromised in any other data breach or unauthorized data disclosure.

88. Plaintiff Nelson suffered actual injury from having her PI exposed as a result of the Unauthorized Data Disclosure including, but not limited to: (a) damages to and diminution in the value of her PI—a form of intangible property; (b) loss of her privacy; and (c) imminent and impending injury arising from the increased risk of fraud and identity theft.

89. As a result of the Unauthorized Data Disclosure, Plaintiff Nelson will continue to be at heightened risk for financial fraud, future identity theft, other forms of fraud, and the attendant damages, for years to come.

**Plaintiff Au**

90. In May 2021, Plaintiff Au received notice from Noblr dated May 14, 2021 ("Notice Letter"). The Notice Letter informed her of the Unauthorized Data Disclosure and that her driver's license number and address may have been accessed. Her husband received a Notice Letter as well as to his own information. Plaintiff Au was not a customer of Noblr and had not requested an insurance quote from Defendant, nor had her husband.

91. Following the Unauthorized Data Disclosure, in January 2021, Plaintiff Au's data was fraudulently used to apply for unemployment benefits in New York. Unemployment fraud is specifically tied to the use of breached driver's license numbers – see paragraphs 47-49 above.

92. As a result, Plaintiff Au contacted the local police department and filed a police report. She also filed a fraud report with New York State Department of Labor.

93. To this day Plaintiff Au's injury prevents her from conducting ordinary

1 business. Before suffering identity theft, she was able to sign into **my.ny.gov** to  
2 file unemployment easily. But now, when she attempts to sign into the “file  
3 unemployment claim” section, she is told there is a different NY.gov username  
4 linked to her social security number. In particular, someone had created a complete  
5 different NY.gov username for NY unemployment. Once the **first** claim was filed  
6 under that fraudulent NY.gov username, her social security number became linked  
7 to that user ID permanently. Plaintiff Au has had no success in reversing or even  
8 stopping the damage she has suffered as a result of the subject Noblr Unauthorized  
9 Data Disclosure. Communications with the unemployment department do not go  
10 through without a passcode for the account. Plaintiff Au has no access to the  
11 passcode to due to the theft of her identity.

12 94. Plaintiff Au researched her options to respond to the theft of her driver’s  
13 license identification and information, and took action including purchasing  
14 IDShield family plan credit monitoring for her and her husband for which she pays a  
15 monthly fee. She spent and continues to spend additional time reviewing her credit  
16 monitoring service results and reports from other online resources concerning the  
17 security of her identity and financial information. This is time Plaintiff Au otherwise  
18 would have spent performing other activities, such as her job and/or leisurely  
19 activities for the enjoyment of life.

20 95. Plaintiff Au has never knowingly transmitted unencrypted PI over the  
21 internet or any other unsecured source. She deletes any and all electronic documents  
22 containing her PI and destroys any documents that contain any of her PI, or that may  
23 contain any information that could otherwise be used to compromise her PI. Plaintiff  
24 Au has not received a notice that her driver’s license number was compromised in  
25 any other data breach or unauthorized data disclosure.

26 96. The identity theft suffered by Plaintiff Sinkwan Au is logically and  
27 temporally linked to the Unauthorized Data Disclosure in the same way that other  
28 data breach cases have found to be “fairly traceable.” Her driver’s license number

1 was stolen shortly before she experienced a fraudulent unemployment claim being  
 2 filed in her name – a form of identity theft specifically linked to stolen driver’s  
 3 license numbers. In most cases, stolen data is rarely attributed to the source when it  
 4 is sold. If sources in darknet markets were named, then law enforcement and ethical  
 5 hackers would immediately notify the company hacked and law enforcement so that  
 6 victims had the opportunity to make the appropriate changes and apply monitoring.  
 7 This makes the stolen data less valuable and less reliable to criminals. Therefore,  
 8 stolen data is often obfuscated, parsed, and sold in pieces. It is also often combined  
 9 with other stolen data, further making attribution to the source very difficult. The  
 10 seller is rarely the original threat actor that performed the exploit. Darknet markets  
 11 and forums rarely allow a market buyer to examine the entire data set before buying  
 12 for obvious reasons. For this reason, case law in many jurisdictions has based its  
 13 “fairly traceable” inquiry on the temporal and logical connections described above.

14 97. Plaintiff Au’s information is for sale on the darknet, as confirmed on  
 15 March 3, 2022, by accessing several Darknet Markets using a trusted identity, which  
 16 found a driver’s license and a student id available for sale in her name on just one of  
 17 these sites. Plaintiff Au’s name is unusual.

18 98. Plaintiff Au suffered actual injury from having her PI exposed as a result  
 19 of the Unauthorized Data Disclosure including, but not limited to: (a) damages to  
 20 and diminution in the value of her PI—a form of intangible property; (b) loss of her  
 21 privacy; and (c) fraud and imminent and impending injury arising from the increased  
 22 risk of further fraud and identity theft.

23 99. As a result of the Unauthorized Data Disclosure, Plaintiff Au will  
 24 continue to be at heightened risk for financial fraud, future identity theft, other forms  
 25 of fraud, and the attendant damages, for years to come.

#### 26 **H. Plaintiffs and Class Members suffered damages**

27 100. Each of the Plaintiffs and Class Members are at risk for actual identity  
 28 theft in addition to all other forms of fraud.

1           101. The ramifications of Noblr’s failure to keep individuals’ PI secure are  
2 long lasting and severe. Once PI is stolen, fraudulent use of that information and  
3 damage to victims may continue for years.<sup>38</sup>

4           102. The PI belonging to Plaintiffs and Class Members is private, valuable and  
5 is sensitive in nature as it can be used to commit a lot of different harms in the hands  
6 of the wrong people. Defendant Noblr failed to obtain Plaintiffs’ and Class  
7 Members’ consent to disclose such PI to any other person as required by applicable  
8 law and industry standards.

9           103. Noblr’s inattention to the possibility that anyone, especially thieves with  
10 various pieces of individuals’ PI, could obtain any individual’s PI who utilized its  
11 front-facing instant quote platform left Plaintiff and Class Members with no ability  
12 to protect their sensitive and private information.

13           104. Noblr had the resources necessary to prevent the Unauthorized Data  
14 Disclosure, but neglected to adequately implement data security measures, despite  
15 its obligations to protect PI of the Plaintiffs and Class Members from unauthorized  
16 disclosure.

17           105. Had Noblr remedied the deficiencies in its data security systems and  
18 adopted security measures recommended by experts in the field, it would have  
19 prevented the intrusions into its systems and, ultimately, the theft of PI.

20           106. As a direct and proximate result of Noblr’s actions and inactions,  
21 Plaintiffs and Class Members have been placed at an imminent, immediate, and  
22 continuing increased risk of harm from identity theft and fraud, requiring them to  
23 take the time which they otherwise would have dedicated to other life demands such  
24 as work and family in an effort to mitigate the actual and potential impact of the  
25

---

26  
27 <sup>38</sup> 2014 LexisNexis *True Cost of Fraud Study*, (August 2014), available at:  
28 <https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf> (last  
visited May 29, 2021).

1 Unauthorized Data Disclosure on their lives.

2 107. The U.S. Department of Justice's Bureau of Justice Statistics found that  
3 "among victims who had personal information used for fraudulent purposes, 29%  
4 spent a month or more resolving problems" and that "resolving the problems caused  
5 by identity theft [could] take more than a year for some victims."<sup>39</sup>

6 108. As a result of Noblr's failures to prevent the Unauthorized Data  
7 Disclosure, Plaintiffs and Class Members have suffered, will suffer, and are at  
8 increased risk of suffering:

- 9 a. The compromise, publication, theft, and/or unauthorized use of their PI,
- 10 b. Out-of-pocket costs associated with the prevention, detection, recovery,  
11 and remediation from identity theft or fraud,
- 12 c. Lost opportunity costs and lost wages associated with efforts expended  
13 and the loss of productivity from addressing and attempting to mitigate the  
14 actual and future consequences of the Unauthorized Data Disclosure,  
15 including but not limited to efforts spent researching how to prevent,  
16 detect, contest, and recover from identity theft and fraud,
- 17 d. The continued risk to their PI, which remains in the possession of Noblr  
18 and is subject to further breaches so long as Noblr fails to undertake  
19 appropriate measures to protect the PI in its possession; and
- 20 e. Current and future costs in terms of time, effort, and money that will be  
21 expended to prevent, detect, contest, remediate, and repair the impact of  
22 the Unauthorized Data Disclosure for the remainder of the lives of  
23 Plaintiffs and Class Members.

---

24  
25  
26  
27 <sup>39</sup> U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics,  
28 *Victims of Identity Theft, 2012*, December 2013, *available at*:  
<https://www.bjs.gov/content/pub/pdf/vit12.pdf> (last visited May 29, 2021).

109. In addition to a remedy for the economic harm, Plaintiffs and the Class Members maintain an undeniable interest in ensuring that their PI is secure, remains secure, and is not subject to further misappropriation and theft.

110. To date, other than providing 12 months of credit monitoring and identity protection services, Noblr does not appear to be taking any measures to assist Plaintiffs and Class Members other than simply telling them to do the following:

- “regularly review statements from your accounts”
- “periodically obtain your credit report”
- “remain vigilant with respect to viewing your account statements and credit reports”
- obtain a copy of a free credit report
- contact the FTC and/or the state Attorney General’s office to obtain additional information about avoiding identity theft

None of these recommendations, however, require Noblr to expend any effort to protect Plaintiffs’ and Class Members’ PI. It is also not clear that Noblr has made any determination that the credit monitoring and identity protection services are designed or adequate to ameliorate the specific harms of having an exposed driver’s license number and address.

111. Noblr’s failure to adequately protect Plaintiffs’ and Class Members’ PI has resulted in Plaintiffs and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money. Instead, as Noblr’s Notice indicates, it is putting the burden on Plaintiffs and Class Members to discover possible fraudulent activity and identity theft.

112. Noblr’s offer of 12 months of identity monitoring and identity protection services to Plaintiffs and Class Members is woefully inadequate. While some harm has begun already, the worst may be yet to come. There may be a time lag between when additional harm occurs versus when it is discovered, and also between when PI

1 is acquired and when it is used.

2 **G. Noblr's delay in identifying and reporting the breach caused additional**  
 3 **harm**

4 113. The actual date Plaintiffs and the Class Members' PI was improperly  
 5 exposed is unknown to Plaintiffs at this time, however, Noblr discovered the  
 6 Unauthorized Data Disclosure on or about January 21, 2021, and it was not until  
 7 almost four months later that Noblr began notifying those affected by the  
 8 Unauthorized Data Disclosure, depriving them of the ability to promptly mitigate  
 9 potential adverse consequences resulting from the Unauthorized Data Disclosure.

10 114. As a result of Noblr's delay in detecting and notifying Plaintiffs and  
 11 Class Members of the Unauthorized Data Disclosure, the risk of fraud for Plaintiffs  
 12 and Class Members has been driven even higher.

13 **CHOICE OF LAW**

14 115. Defendant Noblr is headquartered in San Francisco County, California.  
 15 That is the nerve center of Defendant's business activities—the place where high-  
 16 level officers direct, control, and coordinate Defendant's activities, including data  
 17 security, and where: (a) major policy; (b) advertising; (c) distribution; (d) accounts  
 18 receivable departments; and (e) financial and legal decisions originate.

19 116. Data security assessments and other IT duties related to computer  
 20 systems and data security occur at Defendant's California headquarters.  
 21 Furthermore, Defendant's response, and corporate decisions surrounding such  
 22 response, to the Unauthorized Data Disclosure were made from and in California.  
 23 Finally, Defendant's breach of its duty—including to Plaintiffs and Class and  
 24 Subclass Members—emanated from California.

25 117. It is appropriate to apply California law extraterritorially to the claims  
 26 against Defendant in this case due to Defendant's significant contacts with  
 27 California. Defendant is headquartered in California; the relevant decisions, actions,  
 28 and omissions were made in California; and Defendant cannot claim to be surprised

1 by application of California law to regulate its conduct emanating from California.

2 118. To the extent California law conflicts with the law of any other state that  
3 could apply to Plaintiffs' claims against Defendant, application of California law  
4 would lead to the most predictable result, promote the maintenance of interstate  
5 order, simplify the judicial task, and advance the forum's governmental interest.

### 6 **CLASS ACTION ALLEGATIONS**

7 119. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs  
8 bring this action on behalf of themselves and the following proposed Nationwide  
9 Class (the "Class"), defined as follows:

10 All persons in the United States whose PI was compromised in  
11 the Unauthorized Data Disclosure announced by Noblr on or  
near May 14, 2021.

12 120. Excluded from the proposed Class are any officer or director of  
13 Defendant; any officer or director of any affiliate, parent, or subsidiary of Noblr;  
14 anyone employed by counsel in this action; and any judge to whom this case is  
15 assigned, his or her spouse, and members of the judge's staff.

16 121. **Numerosity.** Members of the proposed Class likely number in at least the  
17 tens of thousands and are thus too numerous to practically join in a single action.  
18 Membership in the Class is readily ascertainable from Defendant's own records.

19 122. **Commonality and Predominance.** Common questions of law and fact  
20 exist as to all proposed Class Members and predominate over questions affecting  
21 only individual Class Members. These common questions include:

- 22 a. Whether Defendant engaged in the wrongful conduct alleged herein,
- 23 b. Whether Defendant's inadequate data security measures were a cause of  
24 the Unauthorized Data Disclosure,
- 25 c. Whether Defendant owed a legal duty to Plaintiffs and the other Class  
26 Members to exercise due care in collecting, storing, and safeguarding their PI,
- 27 d. Whether Defendant negligently or recklessly breached legal duties owed  
28 to Plaintiffs and the other Class Members to exercise due care in collecting, storing,

1 and safeguarding their PI,

2 e. Whether Defendant's online quote system auto-populated prospective  
3 quotes with PI obtained from the records of Defendant or third parties without the  
4 permission or consent of Plaintiffs and the Class,

5 f. Whether Plaintiffs and the Class are at an increased risk for identity theft  
6 because of the data security breach,

7 g. Whether Defendant's conduct violated Cal. Bus. & Prof Code § 17200 *et*  
8 *seq.*,

9 h. Whether Defendant failed to provide timely notice of the Unauthorized  
10 Data Disclosure to Plaintiffs and Class Members in violation of California Civil  
11 Code § 1798.82,

12 i. Whether Defendant violated the Drivers' Privacy Protection Act, 18  
13 U.S.C. § 2724,

14 j. Whether Plaintiffs and the Class Members are entitled to actual,  
15 statutory, or other forms of damages, and other monetary relief, and

16 k. Whether Plaintiffs and the Class Members are entitled to equitable relief,  
17 including, but not limited to, injunctive relief and restitution.

18 123. Defendant engaged in a common course of conduct giving rise to the  
19 legal rights sought to be enforced by Plaintiffs individually and on behalf of the  
20 other Class Members. Similar or identical statutory and common law violations,  
21 business practices, and injuries are involved. Individual questions, if any, pale by  
22 comparison, in both quantity and quality, to the numerous questions that dominate  
23 this action.

24 124. **Typicality:** Plaintiffs' claims are typical of the claims of the members of  
25 the Class. All Class Members were subject to the Unauthorized Data Disclosure and  
26 had their PI accessed by, used and/or disclosed to unauthorized third parties.  
27 Defendant's misconduct impacted all Class Members in the same manner.

28 125. **Adequacy of Representation:** Plaintiffs are adequate representatives of

the Class because their interests do not conflict with the interests of the other Class Members they seek to represent; they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

126. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the Class Members pale compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class Members to individually seek redress for Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

### **FIRST CAUSE OF ACTION**

#### **Violation of the Drivers' Privacy Protection Act ("DPPA"), 18 U.S.C. § 2724 (On behalf of Plaintiffs and the Nationwide Class)**

127. Plaintiffs incorporate the above allegations by reference.

128. The DPPA provides that "[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains." 18 U.S.C. § 2724.

129. Under the DPPA, a "'motor vehicle record' means any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle

1 registration, or identification card issued by a department of motor vehicles.” 18  
 2 U.S.C. § 2725(a). Drivers’ license numbers are motor vehicle records under the  
 3 DPPA. 18 U.S.C. § 2725(3); *see also Dahlstrom v. Sun-Times Media, LLC*, 777  
 4 F.3d 937, 943 (7th Cir. 2015).

5 130. Defendant obtains motor vehicle records from its customers.

6 131. Defendant also obtains motor vehicle records directly from state agencies  
 7 or through resellers who sell such records.

8 132. During the time period up until and including at least January 27, 2021,  
 9 PI, including driver’s license numbers, of Plaintiffs and Class Members, were  
 10 publicly available via query on Noblr’s instant quote webpage and Noblr knowingly  
 11 both used and disclosed Plaintiffs’ and members of the class’s motor vehicle records  
 12 for a purpose not permitted by the DPPA pursuant to 18 U.S.C. §§ 2724 and  
 13 2721(b).

14 133. During the time period up until and including at least January 27, 2021,  
 15 PI, including driver’s license numbers, of Plaintiffs and Class Members, were  
 16 publicly available in the source code of Noblr’s website, Noblr knowingly  
 17 configured its website to make such PI available, and Noblr used and disclosed  
 18 Plaintiffs and Class Members’ motor vehicle records for a purpose not permitted by  
 19 the DPPA pursuant to 18 U.S.C. §§ 2624 and 2721(b).

20 134. Through the Unauthorized Data Disclosure, Defendant disclosed motor  
 21 vehicle records for purposes not authorized by the DPPA.

22 135. Plaintiffs and putative Class Members are entitled to actual damages,  
 23 liquidated damages, punitive damages, attorneys’ fees and costs.

## 24 **SECOND CAUSE OF ACTION**

### 25 **Negligence**

#### 26 **(On behalf of Plaintiffs and the Nationwide Class)**

27 136. Plaintiffs incorporate the above allegations by reference.

28 137. Defendant owed a duty to Plaintiffs and the Class to exercise reasonable

1 care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and  
2 Class Members' PI from being compromised, lost, stolen, and accessed by  
3 unauthorized persons. This duty includes, among other things, designing,  
4 implementing, maintaining and testing its data security systems to ensure that  
5 Plaintiffs' and Class Members' PI in Defendant's possession, or that could be  
6 accessed by Defendant, was adequately secured and protected.

7 138. Defendant owed a duty of care to Plaintiffs and Members of the Class to  
8 provide security, consistent with industry standards, to ensure that its systems and  
9 networks adequately protected PI it stored, maintained, and/or obtained.

10 139. Defendant owed a duty of care to Plaintiffs and Members of the Class  
11 because they were foreseeable and probable victims of any inadequate data security  
12 practices. Defendant knew or should have known of the inherent risks in having its  
13 systems auto-populate online quote requests with private PI and without the consent  
14 or authorization of the person whose PI was being provided.

15 140. Unbeknownst to Plaintiffs and Members of the Class, they were  
16 entrusting Defendant with their PI when Defendant obtained their PI from other  
17 businesses and state motor vehicle databases. Defendant had an obligation to  
18 safeguard their information and was in a position to protect against the harm  
19 suffered by Plaintiffs and Members of the Class as a result of the Unauthorized Data  
20 Disclosure.

21 141. Defendant's own conduct also created a foreseeable risk of harm to  
22 Plaintiffs and Class Members and their PI. Defendant's misconduct included failing  
23 to implement the systems, policies, and procedures necessary to prevent the  
24 Unauthorized Data Disclosure.

25 142. Defendant knew, or should have known, of the risks inherent in  
26 collecting and storing PI and the importance of adequate security. Defendant knew  
27 about – or should have been aware of - numerous, well-publicized unauthorized data  
28 disclosures affecting businesses, especially insurance and financial businesses, in the

1 United States.

2 143. Defendant breached its duties to Plaintiffs and Class Members by failing  
3 to provide fair, reasonable, or adequate computer systems and data security to  
4 safeguard the PI of Plaintiffs and Class Members.

5 144. Because Defendant knew that a breach of its systems would damage  
6 thousands of individuals whose PI was inexplicably stored or was accessible,  
7 including Plaintiffs and Class Members, Defendant had a duty to adequately protect  
8 its data systems and the PI contained and/or accessible therein.

9 145. Defendant also had independent duties under state and federal laws that  
10 required Defendant to reasonably safeguard Plaintiffs' and Class Members' PI.

11 146. In engaging in the negligent acts and omissions as alleged herein, which  
12 permitted thieves to access Noblr's systems that stored and/or had access to  
13 Plaintiffs and Class Members' PI, and which put PI on Noblr's website in a publicly-  
14 available manner through its inclusion in the source code, Defendant violated  
15 Section 5 of the FTC Act, which prohibits "unfair...practices in or affecting  
16 commerce," and the GLB Act. This includes failing to have adequate data security  
17 measures and failing to protect Plaintiffs' and the Class Members' PI.

18 147. Plaintiffs and the Class Members are among the class of persons Section  
19 5 of the FTC and the GLB Act were designed to protect, and the injuries suffered by  
20 Plaintiffs and the Class Members are the types of injury Section 5 of the FTC Act  
21 and the GLB were intended to prevent.

22 148. Neither Plaintiffs nor the other Class Members contributed to the  
23 Unauthorized Data Disclosure as described in this Complaint.

24 149. As a direct and proximate cause of Defendant's conduct, Plaintiffs and  
25 Class Members have suffered and/or will suffer injury and damages, including but  
26 not limited to: (i) the loss of the opportunity to determine for themselves how their  
27 PI is used; (ii) the publication and/or theft of their PI; (iii) out-of-pocket expenses  
28 associated with the prevention, detection, and recovery from unauthorized use of

1 their PI; (iv) lost opportunity costs associated with effort expended and the loss of  
 2 productivity addressing and attempting to mitigate the actual and future  
 3 consequences of the Unauthorized Data Disclosure, including but not limited to  
 4 efforts spent researching how to prevent, detect, contest and recover from tax fraud  
 5 and identity theft; (v) costs associated with placing freezes on credit reports; (vi)  
 6 anxiety, emotional distress, loss of privacy, and other economic and non-economic  
 7 losses; (vii) the continued risk to their PI, which remains in Defendant's possession  
 8 (and/or Defendant has access to) and is subject to further unauthorized disclosures so  
 9 long as Defendant fails to undertake appropriate and adequate measures to protect  
 10 the PI in its continued possession; and, (viii) future costs in terms of time, effort and  
 11 money that will be expended to prevent, detect, contest, and repair the inevitable and  
 12 continuing consequences of compromised PI.

### 13 **THIRD CAUSE OF ACTION**

#### 14 **Violation of the California's Unfair Competition Law**

#### 15 **Cal. Bus. & Prof. Code § 17200, *et seq.***

#### 16 **(Brought by Plaintiffs and the Nationwide Class)**

17 150. Plaintiffs incorporate the above allegations by reference.

18 151. By reason of the conduct alleged herein, Defendant Noblr engaged in  
 19 unlawful and unfair business practices within the meaning of California's Unfair  
 20 Competition Law ("UCL"), Business and Professions Code § 17200, *et seq.*

21 152. Defendant stored and/or provided access to the PI of Plaintiffs and all  
 22 Class Members in its computer systems.

23 153. Defendant knew or should have known it did not employ reasonable,  
 24 industry standard, and appropriate security measures that complied with federal  
 25 regulations and that would have kept Plaintiffs' and all Class Members' PI secure  
 26  
 27  
 28

1 and prevented the loss or misuse of that PI.

## 2 **Unlawful Business Practices**

3 154. Defendant violated the DPPA, Section 5(a) of the FTC Act, the GLB Act  
4 and California Civil Code § 1798.81.5(b) by failing to implement and maintain  
5 reasonable and appropriate security measures or follow industry standards for data  
6 security, and by failing to timely notify Plaintiffs and all Class Members of the  
7 Unauthorized Data Disclosure.

8 155. If Defendant had complied with these legal requirements, Plaintiffs and  
9 the Class Members would not have suffered the damages related to the Unauthorized  
10 Data Disclosure, and Defendant's notification of it.

11 156. Plaintiffs and all Class Members suffered injury in fact and lost money or  
12 property as the result of Defendant's unlawful business practices. In addition,  
13 Plaintiffs and all Class Members' PI was taken and is in the hands of those who will  
14 use it for their own advantage, or is being sold for value, making it clear that the  
15 hacked information is of tangible value. Plaintiffs and all Class Members have also  
16 suffered consequential out of pocket losses for procuring credit freeze or protection  
17 services, identity theft monitoring, and other expenses relating to identity theft losses  
18 or protective measures.

## 19 **Unfair Business Practices**

20 157. Defendant engaged in unfair business practices under the "balancing  
21 test." The harm caused by Defendant's actions and omissions, as described in detail  
22 above, greatly outweigh any perceived utility. Indeed, none of Defendant's actions  
23 or inactions can be said to have had any utility at all. Defendant's failures were  
24 clearly injurious to Plaintiffs and all Class Members, directly causing the harms  
25 alleged below.

26 158. Defendant also engaged in unfair business practices under the "tethering  
27 test." Defendant's actions and omissions, as described in detail above, violated  
28 fundamental public policies expressed by the California Legislature. See, e.g., Cal.

1 Civ. Code § 1798.1 (“The Legislature declares that . . . all individuals have a right of  
 2 privacy in information pertaining to them . . . . The increasing use of computers . . .  
 3 has greatly magnified the potential risk to individual privacy that can occur from the  
 4 maintenance of personal information.”); Cal. Civ. Code § 1798.81.5(a) (“It is the  
 5 intent of the Legislature to ensure that personal information about California  
 6 residents is protected.”); Cal. Bus. & Prof. Code § 22578 (“It is the intent of the  
 7 Legislature that this chapter [including the Online Privacy Protection Act] is a matter  
 8 of statewide concern.”). Defendant’s acts and omissions thus amount to a violation  
 9 of the law.

10 159. Defendant engaged in unfair business practices under the “FTC test.” The  
 11 harm caused by Defendant’s actions and omissions, as described in detail above, is  
 12 substantial in that it affects tens of thousands of Class Members and has caused  
 13 those persons to suffer actual harms. Such harms include a substantial risk of  
 14 identity theft, disclosure of Plaintiffs’ and all Class Members’ PI to third parties  
 15 without their consent, diminution in value of their PI, consequential out of pocket  
 16 losses for procuring credit freeze or protection services, identity theft monitoring,  
 17 and other expenses relating to identity theft losses or protective measures. This harm  
 18 continues given the fact that Plaintiffs’ and all Class Members’ PI remains in  
 19 Defendant’s possession, without adequate protection, and is also in the hands of  
 20 those who obtained it without their consent. Defendant’s actions and omissions  
 21 violated Section 5(a) of the Federal Trade Commission Act. See 15 U.S.C. § 45(n)  
 22 (defining “unfair acts or practices” as those that “cause[ ] or [are] likely to cause  
 23 substantial injury to consumers which [are] not reasonably avoidable by consumers  
 24 themselves and not outweighed by countervailing benefits to consumers or to  
 25 competition”); see also, e.g., *In re LabMD, Inc.*, FTC Docket No. 9357, FTC File  
 26 No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate  
 27 measures to secure personal information collected violated § 5(a) of FTC Act).

28 160. Plaintiffs and all Class Members suffered injury in fact and lost money or

property as the result of Defendant's unfair business practices. Plaintiffs and all Class Members' PI was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiffs and all Class Members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

161. As a result of Defendant's unlawful and unfair business practices in violation of the UCL, Plaintiffs and all Class Members are entitled to equitable and injunctive relief, including restitution or disgorgement.

#### **FOURTH CAUSE OF ACTION**

##### **Declaratory and Injunctive Relief**

##### **(Brought by Plaintiffs and the Nationwide Class)**

162. Plaintiffs incorporate the above allegations by reference.

163. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

164. As previously alleged, Plaintiffs and Class Members had a reasonable expectation that companies such as Defendant, who could access their PI through automated systems, would provide adequate security for that PI.

165. Defendant owes a duty of care to Plaintiffs and Class Members requiring it to adequately secure PI.

166. Defendant still possesses PI regarding Plaintiffs and Class Members.

167. Since the Unauthorized Data Disclosure, Defendant has announced few if any changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Unauthorized Data Disclosure to occur and, thereby, prevent further attacks.

168. The Unauthorized Data Disclosure has caused actual harm because of Defendant's failure to fulfill its duties of care to provide security measures to

1 Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of  
2 additional or further harm due to the exposure of their PI and Defendant's failure to  
3 address the security failings that lead to such exposure.

4 169. There is no reason to believe that Defendant's security measures are any  
5 more adequate now than they were before the Unauthorized Data Disclosure to meet  
6 Defendant's legal duties.

7 170. Plaintiffs, therefore, seek a declaration (1) that Defendant's existing  
8 security measures do not comply with its duties of care to provide adequate security,  
9 and (2) that to comply with its duties of care, Defendant must implement and  
10 maintain reasonable security measures, including, but not limited to:

11 a. Ordering that Defendant engage third-party security auditors/penetration  
12 testers as well as internal security personnel to conduct testing, including simulated  
13 attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and  
14 ordering Defendant to promptly correct any problems or issues detected by such  
15 third-party security auditors,

16 b. Ordering that Defendant engage third-party security auditors and internal  
17 personnel to run automated security monitoring,

18 c. Ordering that Defendant audit, test, and train its security personnel  
19 regarding any new or modified procedures,

20 d. Ordering that Defendant not transmit PI via unencrypted email and not be  
21 permitted to put PI as part of its source code or otherwise be available on its instant  
22 quote webpage,

23 e. Ordering that Defendant not store or make accessible PI in any publicly  
24 facing website,

25 f. Ordering that Defendant purge, delete, and destroy in a reasonably secure  
26 manner customer data not necessary for its provisions of services,

27 g. Ordering that Defendant conduct regular computer system scanning and  
28 security checks, and

h. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a disclosure when it occurs and what to do in response to a breach.

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs, individually, and on behalf of all others similarly situated, respectfully request that the Court enter an order:

- a. Certifying the proposed Class as requested herein,
- b. Appointing Plaintiffs as Class Representatives and undersigned counsel as Class Counsel,
- c. Finding that Defendant engaged in the unlawful conduct as alleged herein,
- d. Granting injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:
  - i. prohibiting Noblr from engaging in the wrongful and unlawful acts described herein,
  - ii. requiring Noblr to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws,
  - iii. requiring Noblr to delete, destroy, and purge the personal information of Plaintiffs and Class Members unless Noblr can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members,
  - iv. requiring Noblr to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal information of Plaintiffs and Class Members' personal information,

- v. prohibiting Noblr from maintaining Plaintiffs' and Class Members' personal information on a cloud-based database,
- vi. requiring Noblr to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Noblr's systems on a periodic basis, and ordering Noblr to promptly correct any problems or issues detected by such third-party security auditors,
- vii. requiring Noblr to engage independent third-party security auditors and internal personnel to run automated security monitoring,
- viii. requiring Noblr to audit, test, and train its security personnel regarding any new or modified procedures,
- ix. requiring Noblr to conduct regular database scanning and securing checks,
- x. requiring Noblr to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal information, as well as protecting the personal information of Plaintiffs and Class Members,
- xi. requiring Noblr to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach,
- xii. requiring Noblr to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Noblr's policies, programs, and systems

- 1 for protecting personal information,
- 2 xiii. requiring Noblr to implement, maintain, regularly review, and revise as
- 3 necessary a threat management program designed to appropriately
- 4 monitor Noblr's information networks for threats, both internal and
- 5 external, and assess whether monitoring tools are appropriately
- 6 configured, tested, and updated,
- 7 xiv. requiring Noblr to meaningfully educate all Class Members about the
- 8 threats that they face as a result of the loss of their confidential personal
- 9 information to third parties, as well as the steps affected individuals
- 10 must take to protect themselves,
- 11 xv. requiring Noblr to design, maintain, and test its computer systems to
- 12 ensure that PI in its possession is adequately secured and protected,
- 13 xvi. requiring Noblr disclose any future data disclosures in a timely and
- 14 accurate manner; and
- 15 xvii. requiring Defendant to provide ongoing credit monitoring and identity
- 16 theft repair services to Class Members.
- 17 e. Awarding Plaintiffs and Class Members damages,
- 18 f. Awarding Plaintiffs and Class Members pre-judgment and post-judgment interest
- 19 on all amounts awarded,
- 20 g. Awarding Plaintiffs and the Class Members reasonable attorneys' fees, costs, and
- 21 expenses; and
- 22 h. Granting such other relief as the Court deems just and proper.
- 23
- 24
- 25
- 26
- 27
- 28

**DEMAND FOR JURY TRIAL**

Plaintiffs, on behalf of themselves and the proposed Class, hereby demand a trial by jury as to all matters so triable.

Dated: March 7, 2022

/s/ Gayle M. Blatt

GAYLE M. BLATT

**CASEY GERRY SCHENK**

**FRANCAVILLA BLATT & PENFIELD, LLP**

David S. Casey, Jr.

*dcasey@cglaw.com*

Gayle M. Blatt

*gmb@cglaw.com*

P. Camille Guerra

*camille@cglaw.com*

110 Laurel Street

San Diego, CA 92101

Telephone: (619) 238-1811

Facsimile: (619) 544-9232

Kate M. Baxter-Kauf (MN #0392037)

\*admitted pro hac vice

Karen Hanson Riebel (MN #0219770)

\*admitted pro hac vice

**LOCKRIDGE GRINDAL NAUEN P.L.L.P.**

100 Washington Avenue South

Suite 2200

Minneapolis, MN 55401

Telephone: (612) 339-6900

Facsimile: (612) 339-0981

*kmbaxter-kauf@locklaw.com*

*khriebel@locklaw.com*